

eGuide: Nie wieder Daten verlieren.

5 Gründe für ein SharePoint Online Backup

Ein Whitepaper zu der
Frage, weshalb eine
Cloud-Backup-Lösung
für SharePoint Online-
Benutzer unverzichtbar
bleibt.

Inhalt

Überblick	3
Einführung	4
SharePoint-Studie: Tun Unternehmen genug für die Datensicherheit in SharePoint? .	5
Welche Folgen hat ein Datenverlust in SharePoint Online?	6
5 Gründe: Warum Datensicherung für Microsoft SharePoint Online unverzichtbar bleibt	7
1. Microsoft erwartet von Ihnen, dass Sie Ihre SharePoint-Daten sichern	7
2. "Menschliches Versagen" ist die Achillesferse von SharePoint	8
3. Gefahr und Folgen von Ransomware-Angriffen	9
4. Compliance und regulatorische Anforderungen	10
5. SharePoint-Daten zu schützen und zu verwalten ist hochkomplex	12
Unterbrechungsfrei arbeiten dank SharePoint Online-Backups	13
5 Gründe, um sich für Keepit zu entscheiden	14
Von Analysten ausgezeichnet und von Kunden geschätzt	15
Technische Bewertung	16
Fazit	16

Überblick

Dieses Whitepaper gibt IT-Fachleuten, SharePoint-Administratoren und CIOs Aufschluss über die fünf wichtigsten Gründe, die zu Datenverlusten in SharePoint Online führen können. Zudem bietet es Empfehlungen, wie Sie diesen (und anderen) Ursachen für Datenverluste entgegenwirken können.

Unternehmen, die geschäftskritische Daten in SharePoint speichern, müssen sich darüber im Klaren sein, dass Microsoft diese Daten nicht schützt. Und sie müssen sich bewusst machen, dass Datenverluste durch Ransomware-Angriffe, menschliches Versagen oder Compliance-Verletzungen hohe Kosten verursachen können. Wussten Sie, dass 49% der Unternehmen in den letzten zwei Jahren eine Datenpanne in ihrer SharePoint-Umgebung erlitten haben?

In diesem Whitepaper erfahren Sie, warum eine Cloud-Backup-Lösung für SharePoint Online unerlässlich ist und welche Kriterien Sie beachten sollten, wenn Sie eine Lösung zum Schutz Ihrer Daten auswählen.

Einführung

SharePoint ist die weltweit beliebteste webbasierte Plattform für Zusammenarbeit und Dokumentenmanagement. Gartner hat SharePoint fünf Jahre in Folge als einen Marktführer im Bereich Content Services-Plattformen eingestuft.

200 Millionen Benutzer weltweit verwenden SharePoint, um Inhalte zu erstellen, zu speichern und im ganzen Unternehmen zu teilen.

SharePoint ermöglicht die Erstellung und Verteilung von Inhalten im Rahmen der Microsoft 365-Suite:

- Manager und Teamleiter benötigen SharePoint zum Management von Projekten und Terminen.
- Verfasser von Inhalten benötigen SharePoint, um Inhalte – Artikel, Präsentationen etc. – zu verfassen, zu veröffentlichen und mit Kollegen zu teilen.
- Wissensarbeiter müssen auf Informationen zugreifen und mit Teams zusammenarbeiten, um ihre Aufgaben erfüllen zu können.
- Führungskräfte benötigen SharePoint, um auf wichtige Informationen zuzugreifen und datengestützte Entscheidungen zu treffen.

Da Unternehmen Microsoft SharePoint in wachsendem Umfang zur Erstellung von Inhalten und zu Kooperationszwecken nutzen, wird die Absicherung der Daten natürlich immer wichtiger – gerade angesichts zunehmender Cyberattacken und Datenverluste.

In diesem Whitepaper beschreiben wir, welche Datensicherheitsvorkehrungen für Microsoft SharePoint Online getroffen werden müssen. Wir zeigen die Sicherheitslücken auf, denen sich Unternehmen aussetzen, wenn sie sich bei der Sicherung, Archivierung und Verwaltung ihrer Daten ausschließlich auf Microsoft ³⁶⁵ verlassen. Und wir erläutern, wie Sie mit Cloud-Backups Zeit und Geld sparen und zugleich Ihren Datenschutzanforderungen gerecht werden können.

SharePoint-Studie: Tun Unternehmen genug für die Sicherheit Ihrer Daten in SharePoint?

Eine **SharePoint-Studie**, die das Ponemon Institute und Metalogix in den USA, im Vereinigten Königreich und in Deutschland durchführten, erbrachte folgende Ergebnisse:

- 49 % der befragten Unternehmen haben in den letzten 2 Jahren Daten in Ihrer SharePoint-Umgebung verloren.
- 84 % der Unternehmen befürchten, dass Zeitarbeiter, Dienstleister oder sonstige Dritte auf Daten zugreifen könnten, zu denen sie keinen Zugang haben sollten.
- 79 % der Unternehmen sind der Ansicht, dass die bestehenden Tools keinen sonderlich guten Schutz vor versehentlicher Datenpreisgabe oder gezielten Verletzungen der Datensicherheit bieten.
- 63 % der Unternehmen haben keinen Überblick darüber, wo sensible Daten gespeichert sind.
- 59 % der Befragten meinen, ihr Unternehmen achte nicht ausreichend darauf, dass SharePoint-Benutzer vertrauliche oder sensible Daten richtig handhaben.
- 63 % der Unternehmen gaben an, dass effektivere Technologien zur Absicherung der Daten erforderlich wären.

SharePoint Data Security

Figure 1. Did your organization have a data breach in the SharePoint environment in the past 2 years?

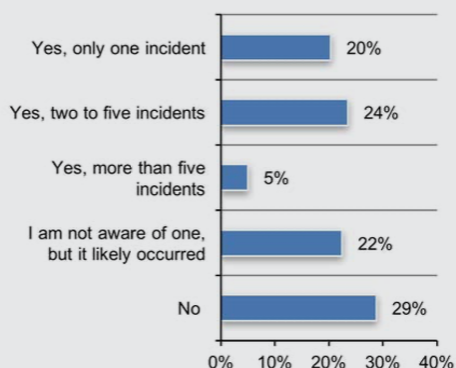
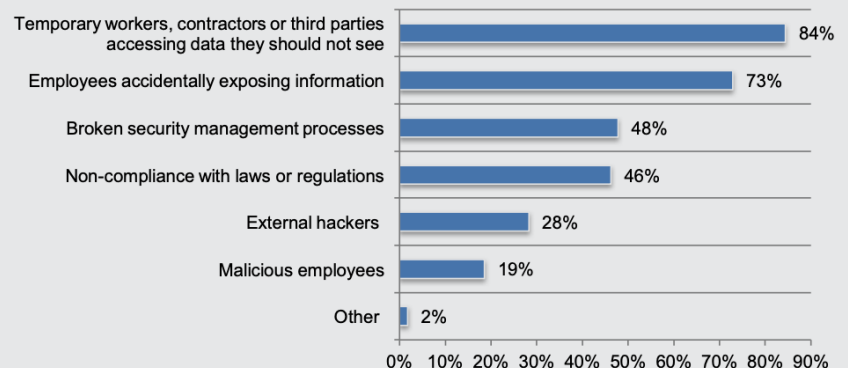


Figure 4. What worries you most about security in the SharePoint environment?
Three choices permitted



Source: Ponemon Institute© Research Report

Welche Folgen hat ein Datenverlust in SharePoint Online?

Ganz gleich, was die Ursache ist, etwa versehentliches oder absichtliches Löschen von Daten durch Mitarbeiter oder ein Ransomware-Angriff: Wenn geschäftskritische SharePoint-Daten verlorengehen, kann dies für ein Unternehmen gravierende Folgen haben. Dazu zählen beispielsweise:

- **Störungen des Geschäftsbetriebs**

In SharePoint werden wichtige Informationen gespeichert, wie etwa Finanzunterlagen, Projektpläne und kundenbezogene Daten. Ein Verlust von SharePoint-Daten kann Ihre Geschäftsabläufe stören, zu Fristversäumnissen führen und die Produktivität beeinträchtigen.

- **Rechtliche Konsequenzen**

Unternehmen, die SharePoint-Daten verwalten, müssen weltweit verschiedenste Datenschutzbestimmungen einhalten, darunter die DSGVO, NIS2, HIPAA, SOX, PCI DSS oder PIPEDA. Andernfalls drohen rechtliche und finanzielle Konsequenzen.

- **Reputationsschäden**

Wenn ein Unternehmen sensible oder vertrauliche Daten verliert – sei es durch einen Mitarbeiterfehler oder die Schuld eines Dritten –, kann sein Ruf Schaden nehmen. Dies wiederum kann das Vertrauen der Kunden und Stakeholder beschädigen und zu Verlusten von Marktanteilen und Umsätzen führen.

- **Wiederherstellungsaufwand**

In SharePoint werden wichtige und sensible Informationen wie Verträge, Finanzplanungen und Kundendaten gespeichert. Gehen solche Daten verloren, kann dies für das Unternehmen kostspielig und zeitraubend werden. Der Arbeitsaufwand für die IT, Ausfallzeiten, Rechts- und Regulierungskosten, Wiederherstellungskosten sowie der Wert der Daten, die vielleicht sogar dauerhaft verloren sind – all dies sind Kostenfaktoren, die auf Sie zukommen können, wenn Sie Ihre Daten nicht aktiv absichern.

5 Gründe: Warum Datensicherung für Microsoft SharePoint Online unverzichtbar ist

1. Microsoft erwartet von Ihnen, dass Sie Ihre SharePoint-Daten sichern

Microsoft ist für den Schutz Ihrer Daten nicht verantwortlich. Ja, Sie haben richtig gelesen: Das Microsoft-Modell der **gemeinsamen Verantwortung** in der Cloud lässt daran keinen Zweifel. Microsoft formuliert dies so:

“Ihre Daten und Identitäten gehören Ihnen. Sie sind für den Schutz der Sicherheit Ihrer Daten und Identitäten, lokalen Ressourcen und der von Ihnen gesteuerten Cloudkomponenten zuständig (abhängig von der Art des Diensts).“

Als Microsoft-Kunde sind Sie also selbst dafür verantwortlich, Ihre Daten und Informationen, Geräte, Konten und Identitäten zu schützen. Das nachfolgende Diagramm veranschaulicht, wie sich die Zuständigkeiten für die Daten verteilen:



Denken Sie daran, dass die Verwendung des Papierkorbs keine tragfähige Backup-Lösung ist. Die Objekte im Papierkorb werden nach 14 Tagen endgültig gelöscht – sich darauf zu verlassen, entspricht also nicht einmal den grundlegenden branchenüblichen Standards für die Sicherung und Wiederherstellung von Daten.

Betriebsstörungen bei Microsoft SharePoint Online oder ein Verlust von SharePoint-Daten können die Geschäftskontinuität Ihres Unternehmens ernsthaft bedrohen. Kein Wunder – schließlich ist ein kontinuierlicher Zugriff auf geschäftskritische Daten unerlässlich.

2. “Menschliches Versagen” ist die Achillesferse von SharePoint

Ransomware gilt seit langem als der mit Abstand größte Risikofaktor für Datenverluste. Tatsächlich sind jedoch Insider-Bedrohungen und menschliches Versagen noch größere Risiken, die Unternehmen einkalkulieren müssen.

Ein **ESG Tech Validation Report** zum Datenschutz bei SaaS zeigt:

- 20 % der SaaS-Datenverluste gehen auf versehentliches Löschen zurück.
- 9 % sind auf Missverständnisse hinsichtlich Aufbewahrungs-/Löschregeln zurückzuführen.
- 8 % der Datenverluste entstehen bei der Schließung von Konten.
- 6 % gehen auf böswillige Löschung durch einen internen Benutzer zurück.

Wenn wir dies kurz überschlagen, stellen wir fest, dass 43 % der SaaS-Datenverluste auf menschliches Versagen zurückzuführen sind.

Wenn Sie durch versehentliches Löschen SharePoint-Daten verlieren, was wird dies Ihr Unternehmen kosten? Oder andersherum gefragt, was ist es Ihnen wert, Ihre Daten zu behalten? Natürlich hängt die Antwort vom Wert des jeweiligen Dokuments ab, doch Datenverluste beschränken sich nun einmal nicht auf Verzichtbares. Nachfolgend sehen Sie, wie SharePoint **in verschiedenen Branchen genutzt wird**:

Gesundheitswesen

Ärzte verwenden SharePoint, um sensible Daten zu speichern und zu verwalten, zum Beispiel Patientenformulare, elektronische Krankenakten, Diagnosebilder, Testergebnisse, Versicherungsunterlagen und Entlassungsberichte. So können sie die Krankengeschichte eines Patienten nachverfolgen und Details zu bestimmten Patienten näher betrachten.

Behörden

Staatliche und kommunale Behörden nutzen SharePoint zur Verwaltung ihrer Dokumente, Projekte und Arbeitsabläufe, um Zeit zu sparen und den Bürgern Dienstleistungen anzubieten.

Bildungseinrichtungen

Bildungseinrichtungen verwenden SharePoint zu Dokumentationszwecken in den verschiedensten Bereichen, wie etwa Finanzen, Forschung, Patente, HR-Kursinhalte und Lehrplanentwicklung, Unterrichtsressourcen und Schüler-/Studentendaten.

Hersteller

Hersteller nutzen SharePoint, um Onboarding- und Schulungsmaterial unternehmensübergreifend auszutauschen, auf Produktionsunterlagen zuzugreifen und Verträge einzusehen.

Bauwesen

Bauunternehmen verwenden SharePoint, um Verträge, Spezifikationen, Zeichnungen und Referenzen zu früheren Projekten für Ausschreibungen zu speichern und Zeitpläne und Fristen aktueller Projekte laufend einsehen zu können. Auch für den Austausch von Dateien mit Kunden, Subunternehmern und Partnern wird SharePoint eingesetzt.

Finanzen und Versicherungen

Banken nutzen SharePoint, um fundierte Entscheidungen treffen zu können, zum Beispiel bei der Genehmigung eines Kredits anhand der Kredithistorie eines Kunden. Sie speichern auch Dokumente und Richtlinien in SharePoint. Versicherungsunternehmen nutzen SharePoint, um die Bearbeitung von Versicherungsfällen zu dokumentieren.

Software

Softwareunternehmen verwenden SharePoint für die Teamarbeit bei der Produktentwicklung, beim Marketing und beim Verkauf von Produkten. Die Erstellung und der Austausch von Inhalten sind dabei wesentliche Elemente.

Wie Sie sehen, ist der Schutz von SharePoint-Daten je nach Branche kein "Nice to have", sondern ein "Must-have", um zu verhindern, dass unbezahlbare, fachspezifische und sensible Daten verlorengehen.

3. Gefahr und Folgen von Ransomware-Angriffen

Angesichts der Häufigkeit von Ransomware-Angriffen lautet die Frage nicht, ob ein Unternehmen angegriffen wird, sondern nur wann. Deshalb müssen Unternehmen vorbeugende Maßnahmen zum Schutz ihrer Daten treffen und Risikomanagementpläne aufstellen.

Die ESG Group hat eine **Ransomware-Studie** durchgeführt, für die IT- und Cybersicherheitsexperten in Unternehmen in Nordamerika und Westeuropa befragt wurden. Hier die Ergebnisse:

- 79 % der befragten Unternehmen hatten im Vorjahr einen Ransomware-Angriff erlebt.
- Jedes sechste Unternehmen wird jede Woche mit Ransomware angegriffen.
- Jedes achte Unternehmen wird täglich mit Ransomware angegriffen.
- 50 % der Unternehmen gaben an, einen Datenverlust erlitten zu haben.
- 40 % gaben an, finanzielle Verluste erlitten zu haben.
- 32 % gaben an, einen Imageschaden erlitten zu haben.
- 30 % gaben an, dass die Compliance gefährdet war.

Ransomware Attack Frequency



Source: ESG Research Report, The Long Road Ahead to Ransomware Preparedness, March 2022

Leider sind dies aber noch nicht alle Folgen von Ransomware. Die bitterste Pille bei dieser Umfrage war, dass 56 % der Unternehmen einräumten, Lösegeld gezahlt zu haben, um wieder auf ihre Daten zugreifen zu können.

Lösegeld zu zahlen, um den Zugang zu Daten zurückzuerhalten, ist riskant und gefährlich. Was würden Sie tun, wenn Ihr Unternehmen diese Woche von einem Ransomware-Angriff betroffen wäre? Benötigen Sie eine Strategie zum Schutz Ihrer Daten?

4. Compliance und regulatorische Anforderungen

Wenn Sie keine Backup- und Datenschutzstrategie für SharePoint Online haben, drohen Bußgelder wegen Nichteinhaltung von Vorschriften und Probleme mit der Datensouveränität. Nachfolgend finden Sie die weltweit wichtigsten Vorschriften, die Sie beachten sollten:

Datenschutz-Grundverordnung (DSGVO):

Die DSGVO regelt, wie personenbezogene Daten in der Europäischen Union verarbeitet und übertragen werden dürfen. SharePoint Online-Daten, die Daten von Personen in der EU enthalten, müssen den Anforderungen der DSGVO entsprechen. Um die DSGVO einzuhalten, müssen Unternehmen entsprechende Datenschutzmaßnahmen umsetzen und die Rechte der betroffenen Personen wahren.

Hier einige Artikel der DSGVO, die Sie besonders zur Kenntnis nehmen sollten:

- Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten, einschließlich der Anforderungen an die Richtigkeit der Daten, die Datenminimierung und Datenaufbewahrung.
- Artikel 32: Sicherheit der Verarbeitung, einschließlich Anforderungen an Verschlüsselung, Zugangskontrollen und die regelmäßige Prüfung und Bewertung der Sicherheitsmaßnahmen.
- Artikel 35: Datenschutz-Folgenabschätzung, wonach Unternehmen eine Abschätzung zu den Auswirkungen treffen müssen, die Datenverarbeitungsvorgänge auf die Privatsphäre von Personen haben können.

Verstöße gegen die DSGVO können für Ihr Unternehmen teuer werden. Hier ein Beispiel:

Marriott International wurde 2018 von der britischen Datenschutzbehörde mit einem Bußgeld in Höhe von 99 Mio. GBP belegt, nachdem ein Cybervorfall aus dem Jahr 2014 ans Licht gekommen war, der mehr als 338 Millionen Datensätze von Gästen betraf.

Sarbanes-Oxley Act (SOX):

SOX ist ein US-Bundesgesetz, das Anforderungen an die Finanzberichterstattung und die Unternehmensführung festlegt. SharePoint Online-Daten, die Finanzinformationen von börsennotierten Unternehmen umfassen, müssen den Anforderungen von SOX entsprechen. Um SOX einzuhalten, müssen Unternehmen Datengenauigkeit gewährleisten, Prüfprotokolle bereitstellen und Sicherheitsmaßnahmen implementieren. Hier einige Artikel von SOX, die Sie bedenken sollten:

- Abschnitt 404 verlangt von Unternehmen, interne Kontrollen über die Finanzberichterstattung einzuführen, einschließlich Kontrollen für die Richtigkeit und Vollständigkeit der Daten.
- Artikel 802 untersagt es, Aufzeichnungen, einschließlich elektronischer, zu verändern, zu vernichten oder zu verfälschen.

Health Insurance Portability and Accountability Act (HIPAA):

HIPAA ist ein Gesetz in den Vereinigten Staaten, das Standards für den Schutz sensibler Gesundheitsdaten von Patienten festlegt. Wenn Ihr Unternehmen im Gesundheitswesen tätig ist und Gesundheitsdaten von Patienten in SharePoint Online speichert, müssen Sie die Anforderungen von HIPAA erfüllen, wie z. B. die Einführung von physischen und technischen Schutzmaßnahmen, die Gewährleistung der Datenintegrität und die Bereitstellung von Zugangskontrollen. Die wichtigsten Vorschriften von HIPAA im Hinblick auf SharePoint Online sind folgende:

- Die Privacy Rule verlangt von den betroffenen Einrichtungen administrative, physische und technische Sicherheitsvorkehrungen zum Schutz elektronisch geschützter Gesundheitsinformationen (ePHI)
- Die Security Rule schreibt den betroffenen Einrichtungen vor, Sicherheitsmaßnahmen zum Schutz von ePHI zu ergreifen, einschließlich Zugriffskontrollen, Verschlüsselung und Audits.
- Die Breach Notification Rule verlangt von den betroffenen Einrichtungen, dass sie im Falle eines Verstoßes gegen ungesicherte ePHI Einzelpersonen, das Department of Health and Human Services und in einigen Fällen auch die Medien benachrichtigen.

NIS2-Richtlinie

Wenn Sie geschäftskritische Daten in SharePoint Online speichern, sollten Sie gegebenenfalls auch die NIS2-Richtlinie beachten.

Am 10. November 2022 (veröffentlicht am 27. Dezember 2022) verabschiedete das EU-Parlament neue Vorschriften zur Stärkung der Cyberresilienz in der gesamten EU.

Die Richtlinie zur Netz- und Informationssicherheit (NIS2) ist eine Reaktion auf die wachsende Gefährdung Europas durch Cyberbedrohungen sowie darauf, dass wir mit zunehmender Vernetzung immer anfälliger für Cyberangriffe werden.

Die NIS2-Richtlinie beinhaltet eine klare Verpflichtung zu Backups und Disaster Recovery-Maßnahmen. Die Richtlinie gilt für folgende Sektoren: Banken und Finanzsektor, Energie, Verkehr, Gesundheitswesen, Trink- und Abwasser, Informations- und Kommunikationsdienstleister, öffentliche Verwaltung und Raumfahrt.

Bei Nichteinhaltung der NIS2-Richtlinie drohen Geldbußen von bis zu 10 Mio. Euro oder 2 % des gesamten weltweiten Jahresumsatzes des jeweiligen Unternehmens. Zudem muss möglicherweise sogar die obere Führungsebene suspendiert werden. [Mehr über die NIS2-Richtlinie erfahren Sie hier.](#)

Payment Card Industry Data Security Standard (PCI DSS):

PCI DSS ist ein Regelwerk zum Schutz von Kreditkartendaten. Wenn Ihr Unternehmen Kreditkartendaten in SharePoint Online bearbeitet oder speichert, müssen Sie den nachstehenden Abschnitt von PCI DSS beachten:

- Abschnitt 802 untersagt es, Aufzeichnungen, einschließlich elektronischer, zu verändern, zu vernichten oder zu verfälschen.

Wenn ein Unternehmen die Compliance- und Datenschutzbestimmungen nicht einhält, drohen rechtliche Konsequenzen und erhebliche Strafen.

5. SharePoint-Daten zu schützen und zu verwalten ist hochkomplex

Der Schutz von SharePoint ist komplex und schwierig. Um SharePoint zu sichern, müssen Sie sämtliche Datenbanken, Anpassungen, Konfigurationen, Einstellungen und Websites sichern. Die Hierarchie ist verschachtelt und kann sehr tief gehen, das heißt, es kann Unterwebsites von Unterwebsites geben.

	Daten einer SharePoint Online-Websitesammlung	Umfasst	Daten mit Cloud-Backup sichern
Listen	Listen mit vererbten Berechtigungen	Elemente, Spalten, Inhaltstypen, Ansichten, Berechtigungen	<i>Keepit sichert diese Daten</i>
	Listen mit eindeutigen Berechtigungen	Elemente, Spalten, Inhaltstypen, Ansichten, Zuweisungen	<i>Keepit sichert diese Daten</i>
	Liste mit einem Element, das eindeutige Berechtigungen hat	Elemente, Elementberechtigungen, Spalten, Inhaltstypen, Ansichten, Berechtigungen	<i>Keepit sichert diese Daten</i>
Dokumentbibliotheken	Dokumentbibliotheken mit vererbten Berechtigungen	Inhalt, Spalten, Inhaltstypen, Ansichten, Berechtigungen	<i>Keepit sichert diese Daten</i>
	Dokumentbibliotheken mit eindeutigen Berechtigungen	Inhalt, Spalten, Inhaltstypen, Ansichten, Zuweisungen	<i>Keepit sichert diese Daten</i>
	Dokumentbibliotheken mit einem Element, das eindeutige Berechtigungen hat	Inhalt, Elementberechtigungen, Spalten, Inhaltstypen, Ansichten, Berechtigungen	<i>Keepit sichert diese Daten</i>
Website-Seiten	Website-Seiten	Inhalte (moderne Website-Seite, Wiki-Seite und Webpart-Seite), Spalten, Inhaltstypen, Ansichten, Listenvorlagen-Galerie, Website-Assets, Berechtigungen, Lösungsgalerie	<i>Keepit sichert diese Daten</i>
	Website-Inhalt	Website-Inhaltstypen	<i>Keepit sichert diese Daten</i>
	Website-Spalten	Websitespalten	<i>Keepit sichert diese Daten</i>
	Berechtigungen	Gruppen, Zuweisungen, Berechtigungsstufen, Website-Administratoren	<i>Keepit sichert diese Daten</i>
	Anpassungen	Schnellstart-Navigationsmenü	<i>Keepit sichert diese Daten</i>
Unterwebsites	Unterwebsites mit vererbten Berechtigungen	Listen, Dokumentbibliotheken, Website-Inhaltstypen, Website-Spalten, Berechtigungen, Unterwebsites	<i>Keepit sichert diese Daten</i>
	Unterwebsites mit eindeutigen Berechtigungen	Listen, Dokumentbibliotheken, Website-Inhaltstypen, Website-Spalten, Berechtigungen	<i>Keepit sichert diese Daten</i>

Unterbrechungsfrei arbeiten dank SharePoint Online-Backups

Es dürfte nun klar sein, dass SharePoint-Daten unbedingt geschützt werden müssen – andernfalls besteht die Gefahr, dass Ihr Unternehmen wichtige Daten verliert, Lösegeldforderungen erhält, Geldbußen für Nichteinhaltung von Vorschriften zahlen muss oder mit sonstigen Problemen durch Datenverluste konfrontiert wird.

Ein Cloud-Backup kann die Auswirkungen von Datenverlusten jeglicher Art minimieren. Mit einem solchen Backup können Sie Ihre SharePoint-Daten sichern, Geschäftskosten einsparen und gleichzeitig den immer strengeren Compliance-Anforderungen gerecht werden. Zu den Vorteilen eines Cloud-Backups zählen folgende:

- Wenn Sie IT- oder SharePoint-Administrator sind, können Sie mit einem Cloud-Backup Daten schnell und zuverlässig zurückgewinnen. Sie haben die beruhigende Gewissheit, dass Ihre SharePoint-Daten im Falle eines gravierenden Datenverlusts sicher und wiederherstellbar sind.
- Wenn Sie CIO oder IT-Leiter sind, hilft Ihnen ein Cloud-Backup, den Disaster Recovery-Plänen Ihres Unternehmens gerecht zu werden und die Sicherheitsvorschriften zu erfüllen, die das Unternehmen einhalten muss.

Wir empfehlen, eine 3-2-1-Datensicherungsstrategie für SharePoint-Daten anzuwenden. Damit können Sie Ihre SharePoint-Daten folgendermaßen schützen:



- 3 Kopien Ihrer Daten: Eine davon sind die Originaldaten in der Produktionsumgebung, die beiden anderen sind Sicherungskopien.
- 2 administrative Bereiche, sodass die Daten unabhängig voneinander in privaten Rechenzentren verwaltet und in logisch getrennten Umgebungen gespeichert werden. Mit diesem Ansatz stehen Ihnen Ihre Daten auch dann zur Verfügung, wenn eine ganze Public Cloud kompromittiert wird.
- 1 Offsite-Kopie außerhalb der Cloud, in der sich die Produktionsumgebung befindet.

Sehen wir uns näher an, wie Ihnen die 3-2-1-Strategie im Fall eines Datenverlusts hilft:

Wenn Sie ein Dokument in SharePoint verlieren, stehen Ihnen zwei Backup-Kopien zur Wiederherstellung zur Verfügung. Werden Ihre Originaldaten in Microsoft 365 gelöscht, überschrieben, beschädigt oder aufgrund von Microsoft Server-Problemen unzugänglich, können Sie auf eine geschützte Datenkopie bei einem unabhängigen Cloud-Backup-Anbieter zurückgreifen.

Ein Cloud-Backup-Anbieter wie Keepit bietet Ihnen eine private, herstellerneutrale Cloud sowie zertifizierte und gespiegelte Rechenzentren. Das gewährleistet, dass Sie jederzeit auf Ihre SharePoint-Daten zugreifen können. Ihr Geschäftsbetrieb wird nicht gestört und Sie verfügen über eine starke Verteidigungslinie gegen Cyberangriffe.

5 Gründe, um sich für Keepit zu entscheiden

- **Einfachheit**

Sparen Sie Zeit mit einer Lösung, die einfach und intuitiv ist – Sie brauchen weder Schulungen noch spezifische IT-Mitarbeiter für die Backups. Die bemerkenswert einfache Wiederherstellung verringert den Zeitaufwand für die Administration, sodass Sie Ihre Daten leicht verwalten und Geschäftskontinuität gewährleisten können.

- **Beste Abdeckung**

Schützen Sie Ihre Daten mit dem besten und detailliertesten Backup für SharePoint Online. Forrester stuft unseren Schutz als „Top Tier“ ein. [Sehen Sie hier alle Daten, die unser Backup sichert.](#)

- **Sofortige Wiederherstellung**

Sie können alle Daten zeit- und mandantenübergreifend finden und schnell wiederherstellen. Wir bieten die beste Auswahl an Wiederherstellungsoptionen für SharePoint-Datensicherungen: In-Place-Wiederherstellung, Wiederherstellung als neue Website mit neuer URL, Wiederherstellung bei einem anderen Mandanten, benutzerübergreifende Wiederherstellung, Download sowie sichere, gemeinsam nutzbare Links.

- **Sicherheit**

Die Architektur von Keepit wurde von Grund auf neu entwickelt. Sie läuft auf einer sicheren, privaten Infrastruktur, die die Unveränderbarkeit und Verfügbarkeit der Daten gewährleistet.

- **Unbegrenzter Speicherplatz**

Keepit bietet Ihnen unbegrenzten Speicherplatz – ein wichtiger Vorteil, wenn Sie große Mengen an Daten in SharePoint haben. Unsere Preisstruktur ist einfach: Dank einer Pauschalgebühr pro Benutzer behalten Sie die Kontrolle über die Kosten. Die Lösung ist leicht skalierbar, verursacht keine versteckten Kosten und beinhaltet Archivierung und unbegrenzte Datenhaltung.

Von Analysten ausgezeichnet und von Kunden geschätzt



Im Forrester New Wave: SaaS Application Data Protection, Q4, 2021, **bewertet Forrester Keepit** als die „beste Lösung für Unternehmen, die Microsoft 365-Schutz und DSGVO-Know-how benötigen“ und stuft Keepit als „Leader“ ein. Forrester würdigte Keepit für:

- Breite Abdeckung
- Gebrauchstauglichkeit
- Sicherheit
- Datenschutz
- Innovative Roadmap

Die Kunden schätzen Keepit wegen seiner Einfachheit, Sicherheit und der schnellen Wiederherstellung. Kunden auf der ganzen Welt bewerten Keepit als hervorragend.

Die **Porsche Holding Salzburg** hat Keepit aus folgenden Gründen für den Schutz vor Ransomware gewählt:

“Immer mehr Unternehmen weltweit sind von Ransomware betroffen. Wir waren auf der Suche nach einer SaaS-Lösung, und wir wollten nicht alle Daten lokal sichern. Dank Keepit haben wir jetzt eine Lösung für den Fall, dass die Porsche Holding je von einem Ransomware-Angriff betroffen sein sollte.”

Andreas Fackler,
Systemingenieur bei
Porsche Informatik, einem
Tochterunternehmen der
Porsche Holding Salzburg

Technische Bewertung

Die ESG (Enterprise Strategy Group) hat eine **technische Bewertung** des SaaS-Datenschutzes durchgeführt, den Keepit bietet. Dabei kam die ESG zu folgendem Schluss:

“Wenn Ihr Unternehmen mit dem Schutz von SaaS-Daten Ernst machen möchte und nach einer Lösung sucht, die einfach, sicher, umfassend und kosteneffizient ist, empfiehlt Ihnen die ESG, sich Keepit genau anzusehen.”

Fazit

Kein Unternehmen, das SharePoint Online-Daten nutzt, kann sich sicher fühlen, ohne über eine Methode zum Schutz dieser Daten zu verfügen. Angesichts der zunehmenden Risiken durch Ransomware-Angriffe, durch versehentliches Löschen von Dateien und durch strengere Strafen bei Compliance-Verstößen ist der Schutz von SharePoint Online-Daten wichtiger als je zuvor. SharePoint-Administratoren, IT-Fachleute und CIOs müssen sich darüber im Klaren sein, dass die Verantwortung für den Schutz der Daten nicht bei Microsoft liegt, sondern bei ihnen selbst. Kein Zweifel: Unternehmen brauchen ein Cloud-Backup zur Wiederherstellung von SharePoint-Daten.

Als Branchenexperte kennt Keepit die Bedürfnisse seiner Kunden und ist bekannt für Einfachheit, Sicherheit und eine schnelle Wiederherstellung.

Erfahren Sie mehr über die dedizierte Lösung von Keepit, mit der Ihr Unternehmen Daten in Microsoft 365, einschließlich SharePoint, zuverlässig schützen kann: **Sehen Sie unsere Produkt-Demo an.**

Über Keepit

Keepit ist die weltweit einzige unabhängige, anbieterneutrale Cloud für den Schutz von SaaS-Daten. Tausende von Unternehmen weltweit vertrauen auf Keepit, um ihre Cloud-Daten zu schützen und zu verwalten.

Führende Analysten sind sich einig: Keepit ist die schnellste und sicherste SaaS-Lösung für Backups und Wiederherstellung in Unternehmen.